TUTORIAL 13

1 Homework 10

1. Assume W is such that $\exists x, x' \in \mathcal{X}, \exists y \in \mathcal{Y}, W(y|x) \neq W(y|x')$. Show that $C(W) > 0$.
2. Show that if C corrects E, then $\exists D : N \to C$ s.t. $\forall x \in C, \forall y \in N, (x, y) \in E \Rightarrow D(y) = x$.

2 Parity check matrix

Let C be a $[n, k, d]_2$-linear code and $G \in \mathbb{F}_2^{k \times n}$ be a generator matrix. That is, $C = \{xG, x \in \mathbb{F}_2^k\}$. We call a parity check matrix of the code C a matrix $H \in \mathbb{F}_2^{(n-k)\times n}$ such that for all $c \in \mathbb{F}_2^n$ we have $cH^T = 0$ if and only if $c \in C$. The objective of this exercise is to show how to construct a parity check matrix from a generator matrix.

1. Show that H is a parity check matrix if and only if $GH^T = 0$ and $\operatorname{rank}(H) = n - k$.
2. Show that, from G we can construct a generator matrix G' of the form $G' = [I_k|P]$ for some $P \in \mathbb{F}_2^{k\times(n-k)}$. (If n is not optimal, we may have to permute the coefficients of the vectors).
3. Construct a parity check matrix from G'.
4. Construct a parity check matrix of the code given by the generator matrix $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ in $\mathbb{F}_2$.

3 Hamming bound

1. Let $0 \leq p \leq \frac{1}{2}$. Give a formula for $\mathrm{Vol}_2(r, n) = |B_2(0, r)|$ the size of the ball in $\mathbb{F}_2^n$ of radius $r = p \cdot n$ where the distance considered is the Hamming weight.
2. Prove the following bound: for any $(n, k, d)_2$ code $C \subseteq (\Sigma)^n$ with $|\Sigma| = 2$,
$$k \leq n - \log_2\left(\mathrm{Vol}_2\left(\frac{d-1}{2}, n\right)\right)$$
3. Define the 2-ary entropy function: $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ defined for $x \in [0, 1]$. Prove that for large enough n, we have: $\mathrm{Vol}_2(pn, n) \leq 2^{nH_2(p)}$.

   Remark. Using Stirling's approximation, we can show that: $\mathrm{Vol}_2(pn, n) \geq 2^{nH_2(p) - o(n)}$ (exercise!).

4 Gilbert-Varshamov bound

1. Let $1 \leq d \leq n$. Show that there exists a (not necessarily linear) $(n, k, d')_2$-code for some $d' \geq d$, such that
$$k \geq n - \log_2\left(\mathrm{Vol}_2\left(d - 1, n\right)\right) .$$

5 Linear Codes Achieving the Gilbert-Varshamov Bound

The purpose of this exercise is to use the probabilistic method to show that a random linear code lies on the Gilbert-Varshamov bound, with high probability.

1. Given a non-zero vector $\mathbf{m} \in \mathbb{F}_2^k$ and a uniformly random $k \times n$ matrix $\mathbf{G}$ over $\mathbb{F}_2$, show that the vector $\mathbf{mG}$ is uniformly distributed over $\mathbb{F}_2^n$.
2. Let $k = (1 - H_2(\delta) - \varepsilon)n$, with $\delta = d/n$. Show that there exists a $k \times n$ matrix $\mathbf{G}$ such that

$$\forall \mathbf{m} \in \mathbb{F}_2^k \setminus \{\mathbf{0}\}, |\mathbf{mG}| \geq d$$

3. Show that $\mathbf{G}$ has full rank (i.e., it has dimension at least $k = (1 - H_2(\delta) - \varepsilon)n$)